

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK



APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

IN RE: Application for a search warrant for
historical cell-site information

19-MC-1266
Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ ☒
Name: Kayla Bensing
Firm Name: U.S. Attorney's Office -- EDNY
Address: 271 Cadman Plaza East
Brooklyn, NY 11201
Phone Number: (718) 254-6279
E-Mail Address: kayla.bensing@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ☒
If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

May 9, 2019
DATE


SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____
Judge/Magistrate Judge: _____
Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK
May 9, 2019
10



U.S. DISTRICT JUDGE/U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE May 9, 2019
DATE

AB:KCB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED CALL
NUMBER 347-424-2280, THAT IS STORED
AT PREMISES CONTROLLED BY T-
MOBILE, AND CALL NUMBER 929-250-
4156, THAT IS STORED AT PREMISES
CONTROLLED BY SPRINT

TO BE FILED UNDER SEAL

**SEARCH WARRANT APPLICATION FOR
HISTORICAL CELL-SITE
INFORMATION**

Case No. 19-MC-1266

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, R. MATTHEW HAMMOND, being first duly sworn, hereby depose and state as
follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number 347-424-2280 (“SUBJECT PHONE 1”), that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054, and a certain telephone assigned call number 929-250-4156 (“SUBJECT PHONE 2”), that is stored at premises controlled by Sprint, a wireless telephone service provider headquartered at 6480 Sprint Pkwy, Overland Park, Kansas, 66251. The information to be searched is described in the following paragraphs and in Attachment A-1 and Attachment A-2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile and Sprint to disclose to the government copies of the information further

described in Section I of Attachments B-1 and B-2, respectively. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review the information to locate items described in Section II of Attachments B-1 and B-2.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since 2007. I am currently assigned to the Violent Crimes Task Force. In that position, I have had significant training and experience investigating a wide range of crimes involving violence and threats of violence, including threats made by telephone, online, and through other electronic means. Through my training, education and experience, I have become familiar with the manner in which crimes involving threats are carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 875(c) (transmitting in interstate or foreign commerce any communication containing any threat to injure the person of another), among other possible violations of law, have been committed by OCTAVIA TELFAIR (the “Subject Offense”). There is also probable cause to search the information described in Attachments A-1 and A-2 for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachments B-1 and B-2.

PROBABLE CAUSE

5. On May 7, 2019, TELFAIR was charged by complaint in the Eastern District of New York of making transmitting in interstate or foreign commerce communications containing any threat to injury the person of another, in violation of 18 U.S.C. § 875(c). The Complaint is currently under seal, is attached as Exhibit 1 and is incorporated by reference herein. Also on May 7, 2019, the Honorable Peggy Kuo, United States Magistrate Judge, signed an arrest warrant (the “Arrest Warrant”) ordering the arrest of TELFAIR. A copy of the Arrest Warrant is attached as Exhibit 2 and incorporated by reference herein.

6. As set forth in the Complaint, following the verdict in her brother, Sebastian Telfair’s, criminal trial on or about April 24, 2019, TELFAIR began placing a series of telephone calls to one of the witnesses in that case, JANE DOE.

7. Specifically, a verdict was rendered in Sebastian Telfair’s trial at approximately 3:30 p.m. Eastern Standard Time (“EST”) on April 24, 2019. Call detail records obtained from the company servicing JANE DOE’s cellular telephone reveal that, on or about April 24, 2019, at approximately 4:27 p.m. EST, SUBJECT PHONE 1 called JANE DOE’s cellular telephone. The same records reveal that, on or about April 24, 2019, at approximately 4:33 p.m. EST, SUBJECT PHONE 1 again called JANE DOE’s cellular telephone. Upon information and belief, JANE DOE answered one or more of the telephone calls from SUBJECT PHONE 1 and recognized TELFAIR’s voice on the phone.

8. Further, call detail records obtained from the company servicing JANE DOE’s cellular telephone reveal that, beginning at approximately 8:58 p.m. EST, SUBJECT PHONE 2 began repeatedly calling JANE DOE’s phone, dozens of times, for a period spanning

approximately two hours. Upon information and belief, JANE DOE answered at least one of the telephone calls from SUBJECT PHONE 2 and recognized TELFAIR's voice on the phone. Further, as set forth in the Complaint, shortly before 8:00 p.m. Pacific Standard Time ("PST"), or approximately 11:00 p.m. EST, JANE DOE recorded a telephone call that she received from TELFAIR. Shortly after the call commences, the video recording of the telephone call reveals that the time of the call is 7:53 p.m. PST. The video recording of the telephone call was approximately 2 minutes and 36 seconds. Call detail records from JANE DOE's telephone reveals that SUBJECT PHONE 2 placed a call to JANE DOE's telephone number at approximately 10:52:59 p.m. EST, and that the duration of that call was approximately 2 minutes and 35 seconds.

9. T-Mobile records show that SUBJECT PHONE 1 was activated on or about May 21, 2018, and that the subscriber name for the account is "OCTAVIA TELFAIR," at an address in the vicinity of Coney Island, Brooklyn. Sprint has not yet responded to a subpoena requesting subscriber and account information for SUBJECT PHONE 2.

VI. The Requested Information

10. The requested information, as more fully described in Attachments B-1 and B-2, would reveal the location of the user of SUBJECT PHONE 1 and SUBJECT PHONE 2, believed to be TELFAIR, close in time to the April 24, 2019 threatening calls made to JANE DOE. In my training and experience, this information may constitute evidence of the Subject Offenses because the information can be used to confirm the SUBJECT PHONE's user and to identify the location of the SUBJECT PHONE and its user in relation to the crime committed against JANE DOE, and it may assist in the identification of coconspirators.

11. In my training and experience, I have learned that T-Mobile and Sprint are companies that provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

12. Based on my training and experience, I know that T-Mobile and Sprint can collect cell-site data about SUBJECT PHONE 1 and SUBJECT PHONE 2. I also know that wireless providers such as T-Mobile and Sprint typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes. I have confirmed that T-Mobile and Sprint are the providers of SUBJECT PHONE 1 and SUBJECT PHONE 2 and possesses the information identified in Attachment B-1.I and B-2.I.

13. Based on my training and experience, I know that wireless providers such as T-Mobile and Sprint typically collect and retain information about their subscribers in their

normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile and Sprint typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify SUBJECT PHONE 1's and SUBJECT PHONE 2's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

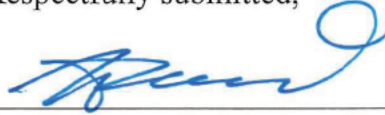
14. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

15. I further request that the Court direct T-Mobile and Sprint to disclose to the government any information described in Section I of Attachments B-1 and B-2 that is within their possession, custody, or control. Because the warrant will be served on T-Mobile and Sprint, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

16. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of

the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,



Special Agent R. Matthew Hammond
Federal Bureau of Investigation

Subscribed and sworn to before me on May ~~7~~⁹, 2019
10



THE HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A-1

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number 347-424-2280 (“the Account”), that is stored at premises controlled by T-Mobile (the “Provider”), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A-1 for the time period between April 15, 2019 through May 8, 2019:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

- vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Section 875(c) (transmitting in interstate or foreign commerce any communication containing any threat to injure the person of another), among other possible violations of law, during the periods between April 15, 2019 through May 8, 2019.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number 929-250-4156 (“the Account”), that is stored at premises controlled by Sprint, a wireless telephone service provider headquartered at 6480 Sprint Pkwy, Overland Park, Kansas, 66251.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A-2 for the time periods between April 15, 2019 through May 8, 2019:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

- vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Section 875(c) (transmitting in interstate or foreign commerce any communication containing any threat to injure the person of another), among other possible violations of law, during the periods between April 15, 2019 through May 8, 2019.